



avast! Mobile Security

Benutzerhandbuch

Inhalt

Willkommen bei avast! Mobile Security	3
Systemanforderungen	4
Die Installation von avast! Free Mobile Security	4
avast! Mobile Security Grundfunktionen	6
Virus Scanner	6
Datenschutz	7
Anwendungs-Management	7
Shield Control	7
SMS- und Anrufilter	9
Firewall - nur auf gerooteten Handys	9
Network-Meter	10
avast! Mobile Security Einstellungen	10
avast! Anti-Theft	12
Die wichtigsten Funktionen von avast! Anti-Theft	12
Selbstgewählter Anwendungsname	14
Grundeinstellungen	15
Erweiterte Einstellungen	16
Unsichtbarer Modus	19
Fernsteuerung	20
Benachrichtigung über SIM-Kartenwechsel	20
Anruf-/SMS Weiterleitung	21
Anrufprotokolle, Kontakte und SMS abfragen	21
Sirene	22
GPS Ortung	22
Selbstschutz	23
Gründliches Löschen	23
Weitere Optionen	24
avast! Anti-Theft deinstallieren	24
avast! Anti-Theft Befehle	25
SMS-Befehlsübersicht	26
avast! Account Internetportal	30

Willkommen bei avast! Mobile Security

avast! Mobile Security ist eine Sicherheitslösung die speziell für Android Geräte entwickelt wurde.

Es besteht aus einem Antivirus zum Schutz ihres Smartphones vor Viren und anderen Schadprogrammen, sowie aus einer Anti-Diebstahllösung mit der Sie, im Fall eines Diebstahles oder Verlustes, Ihr Gerät orten können. Darüber hinaus bietet unser Programm noch Features aus dem Bereich Datenschutz an, mit denen sie zum Beispiel Überwachen können welche Applikationen welche Rechte am Gerät haben. Sie können auch ein- und ausgehende Anrufe und SMS Nachrichten filtern und unerwünschte blockieren.

Der Virenkiller basiert auf bekannten Virensignaturen und wird laufend im Hinblick auf neue Bedrohungen aktualisiert. Auf gerooteten Handys können Sie eine Firewall konfigurieren in der festgelegt wird, wie und ob einzelne Applikationen Zugriff auf das Internet haben.

Mit Anti-Theft können Sie Ihr Telefon mit einfachen SMS Befehlen fernsteuern. So ist es möglich das Gerät zum Beispiel zu Sperren oder eine Sirene zu aktivieren. Darüber hinaus können Sie sich, unsichtbar für den Benutzer, laufend über die aktuelle Position des Handys informieren lassen und ein- wie ausgehende Anrufe und SMS mitverfolgen.

Eins der wichtigsten Features von Anti-Theft ist die Unsichtbarkeit. Wenn es aktiviert ist, ist es am Gerät komplett unsichtbar und ein Dieb würde nicht wissen, dass eine Sicherheitslösung installiert ist. Auch alle ein- und ausgehenden Kommando-SMS sind unsichtbar und hinterlassen keine Spuren am Gerät.

Selbst wenn ein Dieb die Installation entdeckt, kann Anti-Theft nicht so einfach wie andere Anwendungen deinstalliert werden. Wenn die SIM-Karte gewechselt wird, verschickt Anti-Theft eine Benachrichtigungs-SMS mit der neuen Telefonnummer. So können Sie weiterhin Kommando-SMS an das Gerät senden.

avast! Anti-Theft ist eine der am besten versteckten Sicherheitslösungen am Markt!

Systemanforderungen

Für avast! Free Mobile Security muss das System folgende Anforderungen erfüllen.

Unterstützte Betriebssysteme

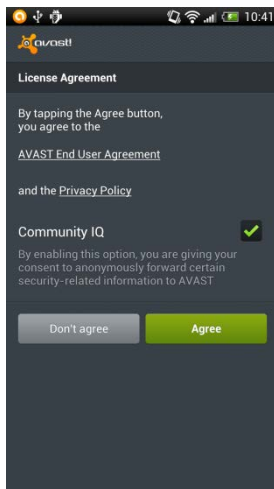
Android 2.1.x, 2.2.x, 2.3.x, 3.x, 4.0.x and 4.x

Mindestanforderungen Hardware

Jedes Telefon mit einem unterstützten Betriebssystem

Die Installation von avast! Free Mobile Security

To install avast! Mobile Security, just download the installation file from Google Play then run the file to install avast! Mobile Security on your phone. Ein einfacher Wizard begleitet sie durch den Installationsprozess.

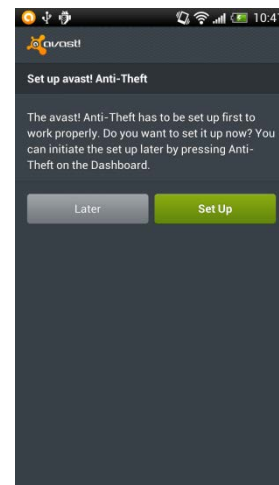


First you will be asked to confirm if you wish to participate in the avast! Community. Diese Option ist vorausgewählt, kann aber abgewählt werden, wenn Sie nicht teilnehmen möchten. Wenn Sie sich entscheiden Teil zu nehmen, werden bestimmte sicherheitsrelevante Informationen an AVAST Software weiter geleitet, die dabei helfen unseren Schutz für alle Benutzer zu verbessern.

Die gleiche Option finden Sie auch in den Anwendungseinstellungen. So können Sie Ihren Teilnahmestatus jederzeit ändern.

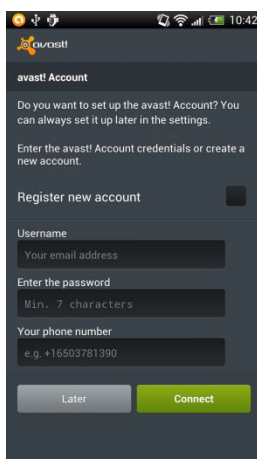
Im nächsten Schritt haben Sie die Möglichkeit das avast! Anti-Theft Feature gleich mitzuinstallieren. Wählen Sie "Installieren" um die Installation zu starten oder "Später" um ohne Anti-Theft Installation fortzufahren. Wenn Anti-Theft nicht gleich mitinstalliert wurde können Sie die Installation später starten, in dem Sie avast! Mobile Security öffnen und im Menü "Anti-Theft" wählen.

Ist die Installation von Anti-Theft gestartet, können Sie zwischen einfachem und fortgeschrittenem Installations-Modus wählen.



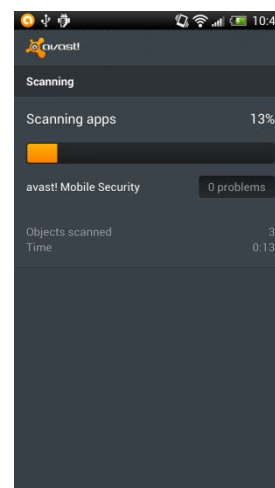
Wenn Ihr Gerät gerootet* ist, haben Sie im "Fortgeschrittenen Installations-Modus" die Möglichkeit Anti-Theft mit root-Rechten zu installieren. Es übersteht damit voll funktionsfähig ein Zurücksetzen des Gerätes auf Werkseinstellungen. Im fortgeschrittenen Installationsmodus können einen eigenen Anwendungsamen für die Anti-Theft-Installation wählen. Natürlich können Sie auch einen der zufällig generierten Vorschläge verwenden. Das ist nützlich, weil im Diebstahlfall nicht offensichtlich eine Sicherheitssoftware entdeckt werden kann.

Bitte beachten Sie, dass Android die Deinstallation von Geräteadministratoren verhindert. Sollten Sie also die Deinstallation von Anti-Theft nicht klappen, prüfen Sie bitte in den Erweiterten Einstellungen unter "Sperrtext, GPS, Löschen" ganz unten "Geräteadministrator" ob die Einstellung noch gesetzt ist.



Im letzten Schritt können Sie Ihr Gerät mit ihrem avast! Konto verbinden oder ein neues erstellen, wenn Sie noch keines haben. Das ist besonders praktisch wenn Anti-Theft installiert ist, weil Sie die Anti-Theft über das Internet, von ihrem avast! Konto aus, steuern können. Diese Funktion wird später im Handbuch, unter "avast! Verwaltungsportal" noch genauer erklärt. Account web portal".

Bestätigen Sie mit "Installieren" Avast! Mobile Security beginnt im Anschluss damit alle bereits installierten Anwendungen zu scannen. Damit wird sichergestellt, dass sich keine Malware am Gerät befindet.

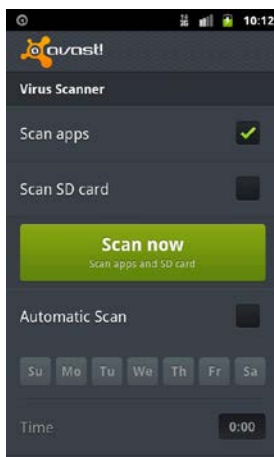


Gerootete Geräte: Sind Handys/Tabs die vom Hersteller - meistens aber vom Benutzer - in die Lage versetzt werden, einzelnen Programmen erhöhte Rechte am Gerät einzuräumen. Weitere Informationen darüber wie sie ihr Gerät rooten können, finden sie mit einer einfachen Internetsuche.

avast! Mobile Security Grundfunktionen

avast! Mobile Security verbessert die Sicherheit Ihres Gerätes mit vielen Features die Ihre Privatsphäre und Daten schützen:

- Virus-Scanner
- Datenschutz
- Anwendungs-Management
- Shield Control
- SMS- und Anrufilter
- Firewall - nur auf gerooteten Handys
- Datenverbrauch
- Anti-Theft
- Einstellungen



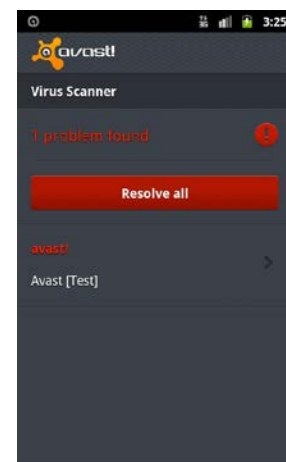
Virus Scanner

avast! Mobile Security scannt auf Befehl alle installierten Anwendungen und/oder den Inhalt der SD-Speicherkarte. Darüber hinaus werden automatisch alle Anwendungen bei ihrer Installation/Update gescannt.

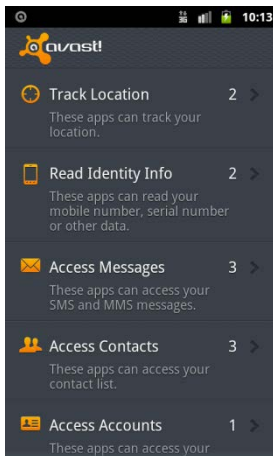
Sie können auch einen automatischen Scan planen - an einem bestimmten Tag (einmal oder mehrmals wöchentlich) zu einer bestimmten Zeit. Beachten Sie, dass für einen geplanten Scan entweder "Apps scannen" oder/und "Scanne Speicherkarte" gewählt sein muss. Wenn etwas verdächtiges gefunden wird, haben Sie die Option die entsprechende Anwendung zu deinstallieren oder die Datei zu löschen.

Wenn etwas verdächtiges gefunden wird, sehen Sie einen roten Knopf im oberen Bildschirmbereich, der sie über das "Problem" informiert. Drücken Sie auf den roten Knopf um zu sehen was entdeckt wurde.

Wenn Sie "Alle erledigen" wählen, werden automatisch alle als schädlich identifizierten Applikationen deinstalliert bzw. Files gelöscht. Sie können auch eine einzelne Anwendung/Dateien wählen. Sie haben dann die Möglichkeit sie zu löschen oder an das avast! Virus Lab als Fehlalarm zu melden, wenn Sie sicher sind, dass die Datei/App in Ordnung ist. Sie helfen uns damit unsere Virus Datenbank zu verbessern und weitere Fehlmeldungen zu verhindern.



Die Virusdefinitionen werden automatisch täglich mehrmals aktualisiert. Es ist aber auch möglich manuell auf Updates zu prüfen.



Datenschutz

Mit avast! Mobile Security können Sie die Zugriffsberechtigungen der installierten Anwendungen prüfen. Sie erhalten eine Aufstellung die Aufschluss darüber gibt, wie viele Anwendungen: Ihre Position bestimmen können, Ihre privaten Daten einsehen, Zugriff auf Ihre Nachrichten haben, Ihre Kontakte und Accounts abfragen können und den Browserverlauf lesen.

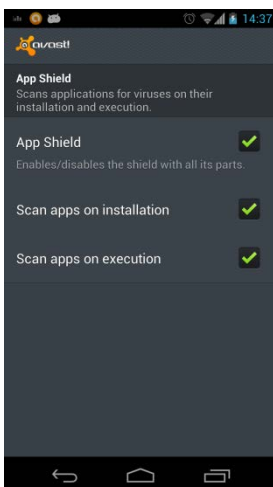
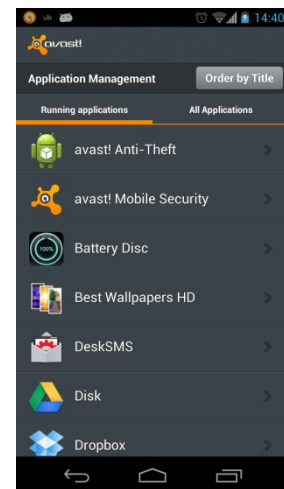
Wenn sie einen der Einträge auswählen, erhalten Sie eine Aufstellung der betroffenen Anwendungen. Das Datenschutz Feature identifiziert also mögliche Risiken die sich aus Kombinationen von Rechten einzelner Anwendungen ergeben können.

Neu Anwendungen werden im Verlauf der Installation auf kritische Rechte geprüft. Sie können dann wählen ob sie mit der Installation fortfahren möchten oder nicht.

Anwendungs-Management

Hier sehen Sie eine Liste aller laufenden Anwendungen. Zu jeder Applikation sehen sie den belegten Speicher (in MB), die momentane CPU Last, den genutzten Hauptspeicher sowie die Summe der Prozesse und Services. Um die Sortierung der Apps zu ändern, drücken Sie bitte auf "Nach Name sortieren" und wählen Sie den gewünschten Parameter.

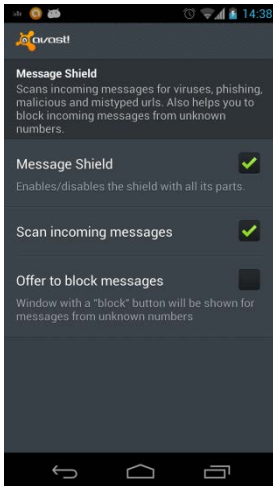
Unter "System-Information" sehen Sie, wieviel Speicher die Anwendung belegt. Sie können eine Applikation auch beenden, in dem Sie "Schliessen erzwingen" wählen. Wenn Sie nach unten scrollen sehen Sie welche Berechtigungen die Anwendung hat (Zugriff auf Daten, Einstellungen etc.)



Shield Control

Hier können Sie die Einstellungen für die verschiedenen Shield-Typen vornehmen.

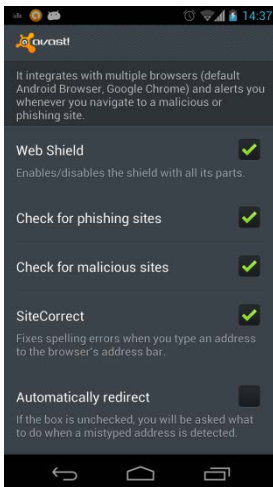
In den **App Shield** Optionen können Sie den Schutz aus und einschalten. Sie können auch Angeben ob Anwendungen bei der Installation oder/und bei jedem App-Start gescannt werden sollen.



Das **Message Shield** bietet folgende Optionen:

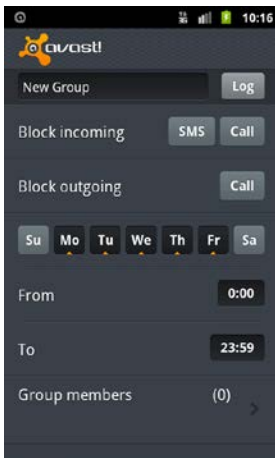
- **Eingehende Nachrichten scannen**
Wählen Sie diese Option um eingehende Nachrichten zu scannen.
- **Nachfrage bei Nachrichtensperre**
Wenn diese Option aktiviert ist, erscheint beim Eingehen einer Nachricht von einem unbekannten Absender ein Fenster. Wenn Sie sich entscheiden zukünftig Nachrichten von diesem Absender zu blockieren, wird "SMS und Anrufilter" geöffnet und sie können eine neue Regel zum Blockieren des Absenders erstellen.

Sie können hier das Message Shield auch komplett ein- und ausschalten.



Der **Web Shield** überprüft jede Webadresse die im Browser geöffnet wird. Wenn eine Adresse als gefährlich eingestuft ist, oder eine bekannte Phishing-Seite öffnet, wird eine Warnung angezeigt. Sie können dann entscheiden ob sie die URL wirklich öffnen, oder auf der aktuell angezeigten Seite bleiben wollen.

- **SiteCorrect**
Wenn Sie sich bei der Eingabe einer Webadresse vertippen, werden Sie gefragt ob Sie nicht lieber die korrekte URL öffnen möchten. So wird zum Beispiel die Eingabe von www.goolge.com auf www.google.com korrigiert.
- **Automatische Umleitung**
Wenn diese Option aktiviert ist, werden Sie automatisch auf korrigierte URLs weitergeleitet. Ist sie deaktiviert, fragt avast! vor jeder Korrektur eines URL-Tippfehlers nach.



SMS- und Anrufilter

Mit avast! Mobile Security können Sie eingehende SMS und Anrufe ihrer Kontakte blockieren. Der Filter basiert auf Regeln und Kontaktgruppen die definieren wann geblockt wird - an einzelnen Wochentagen in der Zeit von - bis. Eine Regel ist also an spezifischen Wochentagen innerhalb des gewählten Zeitraums aktiv.

Sie können eingehende Anrufe und SMS sowie ausgehende Anrufe blockieren. Sie können Wildcards verwenden um Gruppen von Rufnummern zu blockieren. Zum Beispiel blockiert "+4366" alle eingehenden Anrufe bzw. SMS aus Österreich wo der Absender mit 66 beginnt.

Wenn ein Anruf geblockt wird, wird er beendet und im SMS- und Anrufilter Protokoll vermerkt.

Um eine einzelne Nummer oder eine Gruppe von Nummern zu blockieren, müssen Sie erst eine Gruppe erstellen und mit "Neues Gruppenmitglied hinzufügen" die Nummer(n) hinzufügen. Ist eine Gruppe erstellt, können Sie die gewünschten Filter anwenden.

Beachten Sie, dass Nummern mit weniger als vier Stellen nicht geblockt werden können, damit Notrufnummern trotzdem erreicht werden können.



Firewall - nur auf gerooteten Handys

Die avast! Mobile Security Firewall ermöglicht es, auf gerooteten Geräten, einzelnen Anwendungen den Zugriff auf das Internet zu verwehren.

Der Zugriff kann auf einzelne Datenverbindungen beschränkt werden: Sie können den Zugriff auf WiFi, 3G oder Daten-Roaming erlauben/einschränken.



Wählen Sie dieses Icon um 3G Verbindungen zu erlauben.



Wählen Sie dieses Icon um 3G Verbindungen zu erlauben,



und wählen Sie diese Option um Roaming in anderen Netzen zu erlauben.

Es ist auch möglich einzelne Verbindungstypen für Anwendungsgruppen freizugeben.



Network-Meter

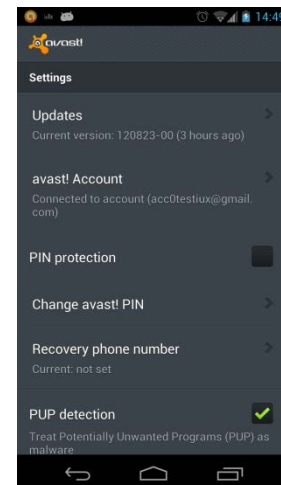
Zeigt das Datenvolumen an, das von Ihrem Smartphone via 3G und/oder WiFi Verbindungen gesendet oder empfangen wird. Wenn Sie eine Anwendung auswählen, sind die Statistiken für Tage, Monate oder das gesamte Jahr verfügbar und erlauben einen direkten Zugriff auf den App-Manager, wenn Sie Änderungen vornehmen möchten.

avast! Mobile Security Einstellungen

Updates

In den Einstellungen sehen Sie die aktuell installierte Version der Virusdefinitionen. Wenn Sie "Updates" auswählen

- **Automatische Updates**
Wenn Sie die Option auswählen wird automatisch bei bestehender Internetverbindung auf verfügbare neue Definitionen geprüft.
- **Verbindungstyp**
Hier können Sie wählen welcher Internetverbindungstyp für die Aktualisierung verwendet werden darf.
- **Jetzt auf Aktualisierungen prüfen**
Wenn Sie diese Option wählen, prüfen Sie manuell auf Aktualisierungen. So können Sie sicherstellen, dass die aktuellsten Virendefinitionen auf Ihrem Gerät verfügbar sind.



avast! Verwaltungsportal

Wenn Sie ein avast! Konto für Ihre avast! Produkte registriert haben, können Sie hier festlegen wie oft Statusmeldungen von Ihrem Gerät an Ihr avast! Konto gesendet werden. Wenn Sie Probleme mit der Verbindung zu Ihrem Konto haben, können Sie mit "Beheben von Verbindungsproblemen" ein Diagnoseprogramm starten. Ist Ihr Gerät hinter einer Firewall, oder wenn Probleme mit der WLAN-Verbindung auftreten, wird das Diagnoseprogramm versuchen den Fehler zu ermitteln.

PIN-Schutz

Hier können Sie den Zugriffsschutz durch Ihre Persönliche Identitäts Nummer (PIN) ein- und ausschalten.

avast! PIN ändern

Wenn ihre avast! Apps PIN-geschützt sind, können Sie hier den PIN ändern.

PIN-Rettungsnummer

Diese Option hilft Ihnen falls Sie einmal Ihren PIN vergessen. In diesem Fall sendet Ihr Gerät eine SMS an die hier angegebene Nummer mit einem PIN der 30 Minuten lang gültig ist. Wenn der PIN in dieser Zeit nicht verwendet wird, wird der original PIN wiederhergestellt.

PUP Erkennung

Ist diese Einstellung gewählt, werden entdeckte potentiell unerwünschte Programme (PUPs) als Malware behandelt.

Datenverbrauch messen

Hier können Sie die Datenverbrauchsmessung deaktivieren. Zum Beispiel um Ihren Batterieverbrauch zu reduzieren.

Prozessor wach halten

Wenn Sie diese Option aktivieren, wird die CPU an einer laufenden Virenprüfung bis zu deren Abschluss weiterarbeiten, auch wenn das Gerät in den Schlafmodus übergeht.

Community IQ

Hier können Sie auswählen, ob Sie der avast! Gemeinschaft beitreten wollen und durch die Übermittlung anonymisierter Nutzungsdaten bei der Weiterentwicklung unserer Software mithelfen möchten.

Benachrichtigungs-Symbol

Hier können Sie die Darstellung des avast! Icons in der Benachrichtigungsleiste einstellen. Sie können zwischen grauer und farbiger Darstellung wählen, oder das Symbol ganz ausschalten. Beachten Sie, dass bei ausgeschaltetem Symbol auch alle avast! Shields deaktiviert sind.

Sprache ändern

Wählen Sie hier die Spracheinstellungen für avast! Mobile Security.

avast! Anti-Theft entfernen

Wenn Sie diese Option wählen wird die Deinstallation von avast! Anti-Theft gestartet, falls Sie die App einst nicht mehr möchten.



avast! Anti-Theft

Wenn Sie Ihr Telefon verlieren oder es gestohlen wird, können Sie es mit avast! Anti-Theft wiederfinden und fernsteuern. Es wird separat installiert, stellt aber einen integrierten Teil von avast! Mobile Security dar. Die Installation erfolgt im Zuge der Installation von avast! Mobile Security oder später als eigene Installation. Wenn die Installation nicht beim installieren von avast! Mobile Security durchgeführt wurde, können Sie die Installation später starten, in dem Sie Anti-Theft im Hauptmenü wählen.

Die Installation von Anti-Theft als eigene App ist erforderlich, damit es am Handy unsichtbar werden kann und so von einem Dieb nicht entdeckt wird. Wenn Anti-Theft aktiviert wird, versteckt es sich automatisch. Diese Funktion ist ein entscheidendes Differenzierungsmerkmal im Vergleich mit anderen Produkten auf Google Play. Andere Anti Diebstahls Apps sind deutlich weniger sinnvoll, weil ein potentieller Dieb der eine Anti-Diebstahlsoftware am Handy findet, das selbe natürlich schnell entsorgt und ein Wiederfinden fast unmöglich wird.

Die wichtigsten Funktionen von avast! Anti-Theft

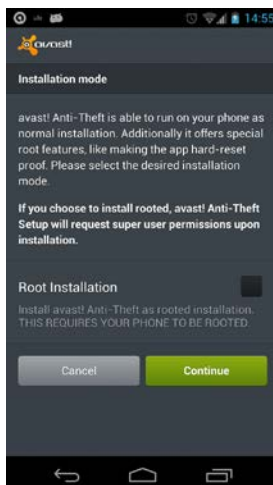
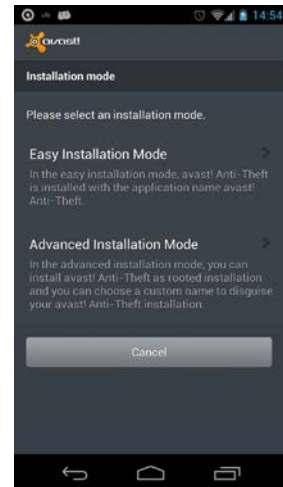
- Benutzer definierter Name - Sie können im Installationsprozess den Namen für die App frei wählen um ihren eigentlichen Zweck zu verschleiern
- Unsichtbarkeit - Die aktivierte Anwendung versteckt sich automatisch damit ein Dieb sie nicht entdeckt
- Fernsteuerung - wenn das Gerät gestohlen wird, können Sie es fernsteuern. Entweder von einem anderen Handy aus, mit SMS-Kommandos, oder über das Internet, wenn Sie sich in Ihr avast!-Konto einloggen
- Nachricht bei SIM-Kartenwechsel - Eine SMS mit der neuen Telefonnummer wird versandt, damit Sie trotzdem noch Kontakt mit dem Handy aufnehmen können
- SMS/Anruf Weiterleitung - Anti-Theft kann auf Wunsch Informationen zu ein- und ausgehenden Anrufen zusenden, Kopien der SMS weiterleiten oder Sie auf Kommando anrufen damit Sie mithören können was im Umfeld passiert.
- Anruf- und SMS-Protokolldaten abrufen - per Befehl können Anrufs- und SMS-Protokolldaten vom Telefon abgefragt werden bevor Sie das Gerät löschen
- Sirene - Das Mobiltelefon beginnt, einen lauten Sirenenton wiederzugeben welcher nur durch einen autorisierten Benutzer wieder deaktiviert werden kann.
- Eigener Sperrtext - Sie können eine eigene Nachricht erstellen die am Screen angezeigt wird wenn das Gerät gesperrt wurde.
- GPS Ortung - GPS kann automatisch aktiviert werden damit Sie sich einmalig oder laufend Ortungsdaten zusenden lassen können
- Selbstschutz - es ist schwierig die Anwendung zu modifizieren oder zu deinstallieren - sie überlebt auf gerooteten Geräten sogar das Zurücksetzen auf Werkseinstellungen

- Gründliches Löschen - Sie können ihr Gerät aus der Ferne löschen um ihre privaten Daten zu schützen.

Selbstgewählter Anwendungsname

Je länger die Anti-Theft Installation von einem Dieb unentdeckt bleibt, um so länger können Sie das Gerät steuern und umso höher sind die Chancen das Handy wieder zu bekommen. Wenn Sie "Fortgeschrittene Installation" wählen, können Sie selbst einen Tarnnamen wählen unter dem sich die Anti-Theft-Installation versteckt. Die Anwendung wird umbenannt um keine Aufmerksamkeit auf sich zu lenken. Man soll nicht merken, dass eine Anti-Diebstahls-Software installiert ist. Sie kann also zum Beispiel "Dodo Gadget" genannt werden.

Das Installationspaket wird auf den gewählten Namen umbenannt und unter diesem Namen als Anwendung installiert. Wenn Sie also in Zukunft nach der Anti-Theft-Installation suchen, halten Sie nach diesem Namen ausschau.



Wenn Ihr Gerät gerootet* ist, haben Sie im "Fortgeschrittenen Installations-Modus" die Möglichkeit Anti-Theft mit root-Rechten zu installieren. Es übersteht damit voll funktionsfähig ein Zurücksetzen des Gerätes auf Werkseinstellungen.

Grundeinstellungen

Nach der Installation müssen Sie die Grundeinstellungen von avast! Anti-Theft vornehmen. Es werden nur wenige Daten benötigt - die Erweiterten Einstellungen sind bereits voreingestellt, können aber nach Ihren Wünschen geändert werden.



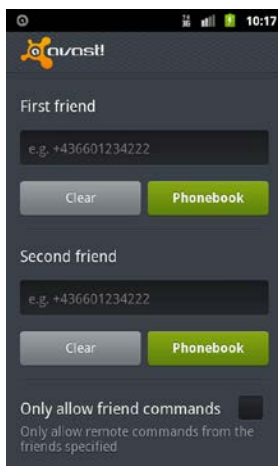
Beginnen Sie, indem Sie sich unter "Ihr Name" als Eigentümer eintragen.

Legen Sie Ihren avast! PIN fest. Er ist eine Zahl mit 4-6 Stellen.

Dieser Zugangs-PIN wird verwendet, um den Zugriff auf Anti-Theft zu erhalten. Vergessen Sie diesen PIN nicht! Ist Anti-Theft einmal aktiviert, ist es aus Sicherheitsgründen im App-Manager nicht mehr sichtbar und kann von dort aus nicht mehr geöffnet werden. Wenn Sie Ihr avast! Passwort anrufen, wie Sie eine Telefonnummer wählen würden, wird der Anruf abgebrochen und das Anti-Theft Menü öffnet sich.

Sie können eine Wiederherstellungshandynummer eingeben. Wenn Sie Ihren avast! PIN vergessen, wird an diese Nummer ein neuer PIN gesendet. Der neue PIN ist 30 Minuten lang gültig. Wird er nicht verwendet, gilt wieder der ursprüngliche PIN.

Der PIN wird auch verwendet, um SMS Kommandos an Ihr Telefon zu autorisieren. Jedes SMS Kommando beginnt mit dem PIN und stellt sicher, dass die eingehende Kommando SMS am Handy nicht angezeigt wird. Ist der PIN falsch, wird die Kommando SMS wie eine herkömmliche SMS als eingehende Nachricht angezeigt.



Abschließend müssen Sie mindestens eine Rufnummer einem Freund oder Familienmitglied angeben, der später SMS-Benachrichtigungen von avast! Anti-Theft erhält.

Wählen Sie "Nur Befehle von Freunden erlauben" damit nur Kommandos von der angegebenen Rufnummer akzeptiert werden.

Anti-Theft ist nun einsatzbereit. Aktivieren Sie Anti-Theft nun in den Grundeinstellungen um Ihr Gerät aktiv zu schützen und es im Verlust- oder Diebstahlfall orten zu können.

Erweiterte Einstellungen

In den erweiterten Einstellungen können Sie festlegen, wie sich avast! Anti-Theft verhalten soll:

1. Schutzverhalten

avast! Anti-Theft führt bestimmte Tätigkeiten automatisch durch, sobald die SIM Karte durch eine unbekannte ersetzt wurde oder Sie den "VERLOREN" Befehl an das Gerät schicken.

Telefon sperren

Ist diese Option aktiviert, wird das Gerät komplett gesperrt. Ein Dieb oder eine sonstige unautorisierte Person daher keinen Zugriff mehr auf das Gerät und kann avast! Anti-Theft auch nicht über den Anwendungsmanager deinstallieren. Der Batterieverbrauch erhöht sich dadurch - aber auch die Sicherheit Ihres Gerätes und der Daten.

Das Gerät kann auch durch das SMS-Kommando "sperren" gesperrt werden.

Sirene einschalten

Wenn diese Option aktiviert ist, ertönt eine Sirene sobald das Gerät gesperrt wird und wird erst stumm, sobald das Gerät wieder entsperrt wird. Die Sirene kann auch über ein SMS Kommando aus- und eingeschaltet werden.

Programm-Manager sperren

Wenn diese Option gewählt ist, kann der Programmmanager nicht geöffnet werden. Wenn das Gerät als "Verloren" markiert ist, oder wenn ein SIM-Kartenwechsel stattgefunden hat, wird der Zugang zum Programmmanager automatisch blockiert.

Telefon-Einstellungen sperren

Wenn diese Option aktiv ist, wird der Zugang zu allen Telefoneinstellungen - inklusive Programmmanager - gesperrt. Wenn das Gerät als "Verloren" markiert ist, oder wenn ein SIM-Kartenwechsel stattgefunden hat, werden die Telefoneinstellungen, samt Programmmanager gesperrt.

USB-Debugging sperren

Zugriff auf die USB-Debugging Schnittstelle sperren damit unautorisierte Personen mit besonderen Werkzeugen keinen Zugriff auf ein gesperrtes Gerät erlangen können.

Datenverbindung erzwingen

Durch aktivieren dieser Option stellen Sie sicher, dass die Datenverbindung eingeschaltet bleibt und die Internetverbindung so lange wie möglich verfügbar ist.

Batterie-Benachrichtigung

Ist diese Option aktiviert, wird automatisch bei niedrigem Batteriestand eine Benachrichtigungs-SMS an die in den Grundeinstellungen als "Freund" angegebene Nummer geschickt. Dadurch ist man gewarnt, bevor der Kontakt zum Handy verloren geht.

2. Sperrtext, GPS, Löschen

Eigener Sperrtext

Hier können Sie einen eigenen Text eingeben der am Sperrbildschirm angezeigt wird (z.B. einen Finderlohn anbieten). Sie können den Text auch bei schon verlorenem Gerät via SMS ändern.

GPS automatisch einschalten

Wenn diese Option gewählt ist, und GPS nicht schon aktiviert ist, wird avast! Anti-Theft versuchen GPS automatisch zu aktivieren um eine genauere Ortung zu ermöglichen. Das geschieht im Fall eines unautorisierten SIM-Kartenwechsels oder wenn ein SMS Kommando eine Ortung auslöst.

Nähere Details finden Sie auf Seite 17.

Gründliches Löschen

Ist diese Option aktiviert, werden beim Ausführen des Löschen-Befehls alle Inhalte auf der SD-Karte unwiederherstellbar gelöscht.

Nähere Informationen finden Sie auf Seite 18.

Geräteadministrator

Sie können hier avast! Anti-Theft als Geräteadministrator einsetzen. Dadurch wird es möglich durch ein Löschen-Kommando das Gerät auf Werkseinstellungen zurückzusetzen.

3. Sirenenton

Die Option "Sounddatei auswählen" öffnet einen Dialog in dem Sie eine Audiodatei auf Ihrem Gerät als Sirenenton auswählen können. Sie können auch eine eigene Audiodatei erstellen mit der Option "Sirenenton aufnehmen". Diese Option wird jedoch auf manchen Geräten nicht unterstützt. Wählen Sie "Sirenenton abspielen" um die aktuell gewählte Sirene abzuspielen oder "Sirene auf Standard" um auf die Standardeinstellung rückzusetzen.

4. Werkseinstellungen überleben

Einstellungen sichern

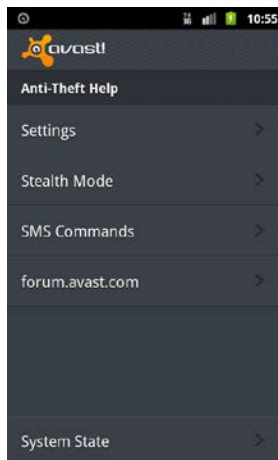
Diese Einstellung ist nur auf gerooteten Geräten verfügbar. Hier können die Anti-Theft-Einstellungen so gespeichert werden, dass sie ein Zurücksetzen auf Werkseinstellungen des Gerätes überstehen.

Einstellungen überprüfen

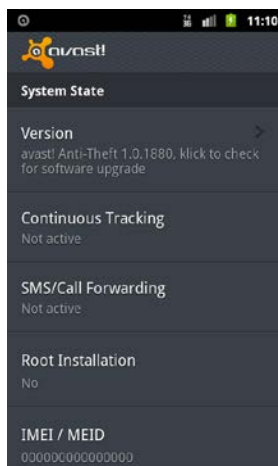
Hier können Sie prüfen, ob die Einstellungen korrekt gespeichert wurden.

5. Software-Aktualisierungen

Wenn Sie unter "Systemstatus" den Eintrag "Version" wählen, können Sie prüfen ob die aktuellste Version von avast! Anti-Theft installiert ist. Ihr Gerät kann auch eine automatische wöchentliche Prüfung durchführen, um sicherzustellen dass immer die aktuelle Version installiert ist. Diese automatische Prüfung erfolgt nur, solange eine vertrauenswürdige SIM Karte eingesetzt ist und das Gerät nicht als "verloren" markiert wurde.



Wählen Sie **Hilfe, Systemstatus, Info** im unteren Menübereich um Zugriff auf die Hilfe zu erhalten. Sie finden dort Erklärungen zum Programm sowie eine Liste der verfügbaren SMS Kommandos...



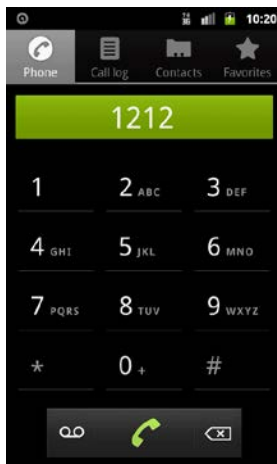
...und wenn Sie System Status wählen, sehen Sie alle momentan aktiven avast! Systemeinstellungen wie zum Beispiel GPS Tracking, SMS/Anrufweiterleitung, ob GPS Autoaktivieren aktiv ist usw. Diese Funktionen werden auf den folgenden Seiten beschrieben.

Unsichtbarer Modus

Eine spezielle Eigenschaft von Anti-Theft ist der sogenannte unsichtbare Modus. Anti-Theft ist der einzige Diebstahlschutz am Markt der sich selbst aktiv auf dem Gerät versteckt. Dadurch steigt die Chance, Diebe zu schnappen oder zumindest das Gerät zurückzubekommen.

Diebe prüfen gestohlene Geräte üblicherweise auf Anwendungen die ihre Identität aufdecken könnten. Sie suchen nach Anwendungslogos und durchsuchen die Anwendungsliste. Wenn ein Dieb eine solche Anwendung findet, ist es sehr wahrscheinlich, dass das Gerät ausgeschaltet und entsorgt wird. Dadurch kann das Gerät üblicherweise nicht mehr gefunden werden.

Anti-Theft versteckt sich, in dem ein falscher Anwendungsname für die Installation verwendet wird. Darüber hinaus scheint die Anwendung nicht in der Programmliste auf und ist so komplett unsichtbar.



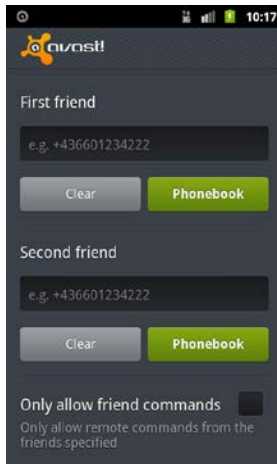
Im unsichtbaren Modus können Sie Anti-Theft nicht wie andere Anwendungen starten, weil es eben unsichtbar ist. Sie können die Anti-Theft Oberfläche starten, in dem Sie **ihren avast! PIN anrufen** - wie Sie es mit einer herkömmlichen Telefonnummer tun würden. Ist Ihr avast! Pin zum Beispiel 1212, machen Sie einen Anruf an die Nummer 1212. Der Anruf wird unterbrochen ohne Kosten zu verursachen und Anti-Theft wird gestartet.

Um Anti-Theft in der Programmliste wieder sichtbar zu machen, schalten Sie den Anti-Theft Schutz in den Grundeinstellungen aus. Dadurch wird der Eintrag im Programmmenü wieder sichtbar geschaltet.

Auf Tablets, die keine Telefonanwendung installiert haben, können Sie die Oberfläche über Ihr avast! Konto am Webportal öffnen.

Fernsteuerung

Um später Verbindung zu Ihrem Gerät herzustellen, können Sie nun bis zu zwei Benachrichtigungsnummern für avast! Anti-Theft registrieren. Zum Beispiel ihr zweites Telefon und die Nummer eines Freundes oder Familienmitglieds.



Geht das Gerät verloren oder wird es gestohlen, empfangen diese Nummern alle Nachrichten die avast! Anti-Theft vom verlorenen Gerät aus verschickt. Sie können auch von jedem anderen Handy aus SMS Kommandos an das verlorene Gerät schicken und am Absenderhandy Antworten empfangen. Wenn Sie aber "Nur SMS Befehle von Freunden erlauben" wählen, werden nur von den beiden registrierten Nummern empfangene Kommandos ausgeführt. Um diese Einschränkung wieder zu entfernen, können Sie diese Option auch wieder abwählen.

Mit den SMS Kommandos können sie, am verlustigen Gerät unbemerkt, Details zu aus- und eingehenden Anrufen abfragen, Kopien von ein- und ausgehenden SMS Nachrichten lesen, das Gerät sperren oder sogar aus der Ferne alle persönlichen Daten löschen wenn Sie nicht mehr damit rechnen das Gerät wieder zurück zu bekommen. Sie können sich auch laufende GPS Ortungen zuschicken lassen um das Gerät zu verfolgen. Alle verfügbaren SMS Kommandos werden später in diesem Handbuch genauer erklärt.

Benachrichtigung über SIM-Kartenwechsel

In der Regel wird bei einem gestohlenen Gerät der Dieb nach einiger Zeit die SIM-Karte wechseln. Die neue Telefonnummer ist dem eigentlichen Besitzer dann nicht mehr bekannt und es können keine weiteren SMS Kommandos gesendet werden. avast! Anti-Theft erkennt aber unautorisierte SIM-Kartenwechsel und sendet ihnen dann die neue Nummer und eine aktuelle Ortung an die von Ihnen registrierte Nummer eines Freundes oder Familienmitglieds. Die Absendernummer der SMS ist dabei die Telefonnummer der SIM die im Handy eingelegt ist. Anti-Theft wird die aktuelle Position des Handys in der SMS als Link zu einer Karte mit eingezeichneter Position schicken.

Sie können prüfen ob die Benachrichtigungsnummern korrekt eingegeben wurden in dem Sie im Hauptmenü auf den Menü-Knopf drücken und "Test-SMS senden" wählen. Wenn alles korrekt konfiguriert ist, wird eine Test-SMS an die Nummer(n) gesendet, die in den Grundeinstellungen eingegeben wurden.

Sie können über eine Option in den erweiterten Einstellungen festlegen, dass Ihr Gerät, im Fall eines unautorisierten SIM-Kartenwechsels, automatisch gesperrt wird (optional auch mit Sirene). Diese Einstellung schützt Ihre persönlichen Daten am Gerät, würde aber einen Dieb auf die installierte Anti-Diebstahllösung aufmerksam machen. Diese Funktion kann getestet werden, in dem Sie im Hauptmenü auf den Menüknopf und "Sperrung simulieren" drücken.

Sie können in avast! Anti-Theft auch mehrere SIM-Karten als vertrauenswürdig registrieren. Die jeweils aktuell eingelegte SIM Karte wird zur Liste vertrauenswürdiger SIM Karten hinzugefügt, wenn die Anti-Theft-Oberfläche geöffnet wird. Bevor Sie eine neue SIM Karte hinzuzufügen, deaktivieren Sie die automatische Sperrfunktion. Schalten Sie das Gerät dann aus und wechseln Sie die SIM-Karte wie gewohnt. Nachdem Sie das Handy wieder eingeschaltet haben, starten Sie die Anti-Theft Oberfläche und die neue SIM Karte wird automatisch als vertrauenswürdig erkannt.

Sie können die Liste der vertrauenswürdigen SIM Karten jederzeit wieder löschen indem Sie im Hauptmenü auf den Menüknopf und "SIM-Liste löschen" drücken. Damit wird die aktuell eingelegte SIM-Karte zur einzig vertrauenswürdigen.

Anruf-/SMS Weiterleitung

Mit avast! Anti Theft können, über ein SMS Kommando, eingehende Anrufe und SMS an ein anderes Gerät weitergeleitet/kopiert werden.

Anrufe: bei jedem eingehenden Anruf am verlustigen Gerät werden per SMS Informationen über den Anruf an ein anderes Handy versandt. Der Anruf selbst wird NICHT weitergeleitet.

SMS: wenn eine SMS am verlorenen Handy eingeht, kann es entweder weitergeleitet und gelöscht werden (dann erscheint die SMS erst gar nicht am verlorenen Gerät) oder, je nach Befehl, weitergeleitet und am Handy angezeigt werden.

Sie können mit dem "RUF AN" Befehl auch einen versteckten Anruf auslösen. Das verlorene Handy ruft Sie dann an, und Sie können unauffällig mithören was am anderen Ende der Leitung passiert.

Anrufprotokolle, Kontakte und SMS abfragen

Mit einem einfachen SMS Kommando kann man eine Abfrage des Anrufprotokolls, der Kontakte und der am Handy gespeicherten SMS starten. Jeder Kontakt, SMS und Anrufeintrag wird als einzelne SMS an das abfragende Handy geschickt. Es ist möglich auf bestimmte Telefonnummern zu filtern, die Anzahl abgefragter gesendeter/empfangener SMS usw. zu begrenzen, um die Anzahl der Abfrage-SMS zu begrenzen. Dadurch kann man noch wichtige Daten retten, bevor man das Gerät löscht.

Sirene

Mit Anti-Theft kann man, mit einer einfache SMS ferngesteuert, eine laute Sirene am Gerät ein- und ausschalten. Solange das Gerät eingeschaltet ist, wird die Sirene laufen. Wenn am Gerät die Lautstärke reduziert wird, stellt Anti-Theft die Lautstärke nach einem kurzen Moment wieder auf das Maximum ein. Die Sirene kann auch personalisiert werden in dem ein eigener Sirenton aufgenommen wird oder eine Audio-Datei am Handy ausgewählt wird.

GPS Ortung

Wie bereits erwähnt, erkennt Anti-Theft unautorisierte SIM-Kartenwechsel und sendet automatisch die neuen Nummer an den Freund bzw. Familienangehörigen dessen Nummer(n) man angegeben hat. Wenn GPS aktiviert ist, beinhaltet diese SMS auch GPS Ortungsdaten. Mit dem SMS Kommando "ORTEN" kann der Versand einer Ortungs-SMS manuell ausgelöst werden. Sie können die Ortung einmalig, oder mit einer definierten Frequenz laufend anfordern.

In den erweiterten Einstellungen können Sie mit der Option "GPS automatisch einschalten" die GPS Funktion Ihres Gerätes automatisch aktivieren wenn ein Ortungsbefehl eingeht.

Beachten Sie, dass bei Ortungsbefehlen GPS immer automatisch eingeschaltet wird, wenn das Gerät gerootet ist. Auf nicht gerooteten Geräten gibt es hier Einschränkungen. Die automatische Aktivierung von GPS funktioniert auf nicht gerooteten Geräten nur von Android 1.6 bis Android 2.2. Auf Geräten mit Android 2.3 und neuer ist es nicht möglich GPS für Ortungen automatisch zu aktivieren.

Auf manchen nicht gerooteten Geräten öffnet die automatische GPS Aktivierung auch unerwünschte Dialoge. Deshalb kann man auf nicht gerooteten Geräten wählen, ob man GPS automatisch aktivieren möchte, oder nicht.

Um zu prüfen, ob auf Ihrem Gerät solche Dialoge aufgehen, aktivieren Sie bitte "GPS automatisch einschalten" und deaktivieren Sie die GPS Funktionalität in den Einstellungen Ihres Handys. Öffnen Sie nun Anti-Theft, drücken den Menüknopf und wählen "Diebstahl simulieren". Wenn ein Fenster aufgeht, empfehlen wir diese Einstellung zu deaktivieren um keine Aufmerksamkeit auf die Anti-Theft Installation zu lenken.

Beachten Sie, dass "GPS automatisch aktivieren" keinen laufenden Batterieverbrauch verursacht. Die GPS Funktion wird nur für den Moment aktiviert in dem sie tatsächlich zum Orten benötigt wird. Es wird also nur Strom verbraucht, wenn das GPS tatsächlich aktiviert ist.

Selbstschutz

Anti-Theft unternimmt alles um sich möglichst gut zu schützen - das gelingt auf gerooteten Geräten am besten. Auf gerooteten Geräten versteckt und tarnt sich Anti-Theft nicht nur, es kann auch nicht so einfach deinstalliert werden und überlebt sogar ein Zurücksetzen auf Werkseinstellungen (=Hardreset) des Geräts.

Damit das klappt, reicht es aber nicht Anti-Theft gerootet zu installieren, weil die Anwendung zwar überleben würde, die Einstellungen aber gelöscht würden.

Man muss daher auch die Einstellungen im root-Modus speichern. Wenn man Anti-Theft fertig konfiguriert hat, muss man als letzten Schritt die Einstellungen hard reset sicher abspeichern. Man öffnet dazu die erweiterten Einstellungen -> Werkseinstellungen überleben -> Einstellungen sichern. Der Sicherungsvorgang ist als Dialog gestaltet und recht einfach. Wichtig ist, dass man nach jeder Änderung der Einstellungen von Anti-Theft wieder hard reset sicher speichert, damit die Änderungen im Fall des Zurücksetzens auf Werkseinstellungen nicht verloren gehen.

Innerhalb der erweiterten Einstellungen gibt es weitere "Schutzverhalten"-Einstellungen, mit denen festgelegt wird, wie avast! Anti-Theft sich im Fall, dass die SIM-Karte mit einem neuen, unbekannten SIM-Karte ausgetauscht wird, oder wenn das Telefon als "verloren" markiert wird, verhält. Zum Beispiel kann das Telefon, der Zugriff auf den Programm-Manager, die Telefoneinstellungen oder der USB Zugriff gesperrt werden. Man kann auch das Offenhalten der Datenverbindung erzwingen.

Ab Android 2.2 ist es möglich avast! Anti-Theft als Geräteadministrator einzusetzen. Solange diese die Geräteadministratoreinstellung aktiv ist, KANN ANTI-THEFT NICHT DEINSTALLIERT WERDEN.

Gründliches Löschen

Das Handy kann via SMS Kommando gelöscht werden, wenn Sie nicht mehr erwarten, dass sie das Gerät wieder zurückbekommen und nicht möchten, dass jemand Zugriff auf Ihre gespeicherten persönlichen Daten hat.

Bis Android 2.1 ist das Löschen nur eingeschränkt möglich, weil ein Zurücksetzen auf Werkseinstellungen nicht möglich ist. Anti-Theft wird aber trotzdem versuchen, möglichst viele Daten zu löschen. Unter anderem Kontakte, Anrufprotokolle, SMS/MMS, Browserverlauf und SD-Karteninhalte. Emails und Apps können aber nicht gelöscht werden.

Ab Android 2.2 kann man das Gerät auf Werkseinstellungen zurück setzen - so können alle Daten gelöscht werden. Beachten Sie, dass damit auch avast! Anti-Theft gelöscht wird - sofern es nicht gerootet installiert ist. Damit das SMS Kommando "löschen" ihr Gerät auf Werkseinstellungen zurücksetzen kann, muss Anti-Theft in den erweiterten Einstellungen als Geräteadministrator eingesetzt werden, sonst können Anwendungen, E-Mails etc nicht gelöscht werden.

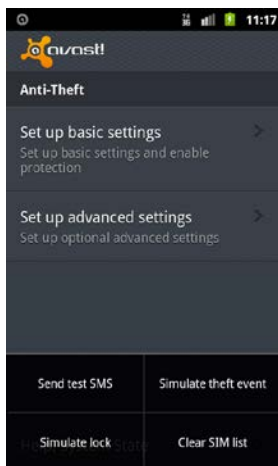
Immer wenn mit Anti-Theft ein Gerät gelöscht wird, werden auch die SD Karteninhalte gelöscht. Im Rahmen eines Standardlöschvorgangs werden die Dateien und Verzeichnisse gelöscht. Das geht am schnellsten, aber erfahrene Diebe können die Daten mit besonderen Werkzeugen wiederherstellen.

Das "gründliche Löschen" dauert bis zu 10 Minuten, dabei werden aber physisch und unwiederherstellbar die SD-Karteninhalte gelöscht. Es ist Ihre Wahl ob Sie das Maximum an Sicherheit wünschen oder ob eine schnelle Durchführung des Löschvorgangs für Sie wichtiger ist.

Weitere Optionen

Sie können mit Anti-Theft verschiedene Tests durchführen um sicherzustellen, dass Ihre Anti-Theft Installation korrekt konfiguriert ist und entsprechend Ihren Vorstellungen agiert.

Sie erhalten Zugang zu diesen Optionen, wenn sie den Menü-Knopf drücken.



Test-SMS senden - sendet, auf Ihrem Gerät unsichtbar, eine SMS an die Nummern die Sie als "Freunde" in den Grundeinstellungen festgelegt haben.

Sperrre simulieren - simuliert das "sperren"-SMS-Kommando. Das Gerät wird dabei für 10 Sekunden gesperrt.

Diebstahl simulieren - alle Aktionen werden ausgeführt, die im Fall eines unautorisierten SIM-Kartenwechsels, oder wenn das Gerät als "verloren" markiert wird, durchgeführt werden sollen. Unter anderem wird eine SMS an die angegebenen Nummern der Freunde geschickt. Das kann ein bisschen dauern, weil vorher eine Ortung durchgeführt wird.

SIM-Liste löschen

avast! Anti-Theft deinstallieren

Für gewöhnlich kann avast! Anti-Theft sehr einfach über den Programmmanager deinstalliert werden. Einfach avast! Anti-Theft wählen, "System Info" wählen und deinstallieren.

Beachten Sie, dass Android die Deinstallation von Geräteadministratoren nicht erlaubt. Sollte die Deinstallation von Anti-Theft nicht klappen, prüfen Sie bitte in den Erweiterten Einstellungen unter "Sperrtext, GPS, Löschen", ganz unten "Geräteadministrator", ob die Einstellung noch gesetzt ist. Entfernen Sie die Einstellung und deinstallieren Sie wie üblich.

avast! Anti-Theft Befehle

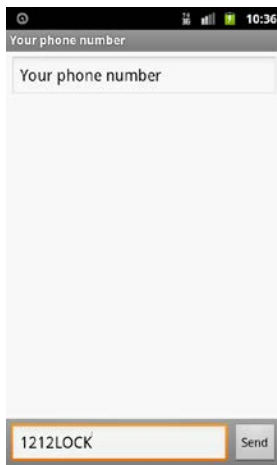
Mit avast! Anti-Theft können Sie Ihr Gerät mit einfachen SMS Befehlen fernsteuern. Dazu muss der Anti-Theft Schutz in den Anti-Theft Grundeinstellungen eingeschaltet sein.

Anti-Theft Befehle können von jedem anderen Mobiltelefon aus gesendet werden, das SMS versenden kann.

Wenn Sie in den Fernsteuer-Einstellungen angegeben haben, dass nur Freunde SMS-Befehle senden dürfen, werden SMS-Befehle nur von den in den Fernsteuer-Einstellungen als Freunde spezifizierten Telefonnummern akzeptiert. SMS-Befehle von anderen Nummern werden dann ignoriert.

Für eine komplette Übersicht über alle SMS Befehle auf ihrem Gerät öffnen Sie die Anti-Theft Hilfe und wählen Sie "SMS-Befehle"

SMS BEFEHLE



Alle SMS-Befehle müssen mit Ihrem avast!-PIN beginnen. Wenn der avast! PIN beispielsweise auf 2222 gesetzt wurde, muss ein Sperrbefehl wie folgt aussehen: 2222 SPERREN

Wenn Sie in den Fernsteuer-Einstellungen angegeben haben, dass nur Freunde SMS-Befehle senden dürfen, werden SMS-Befehle nur von den in den Fernsteuer-Einstellungen als Freunde spezifizierten Telefonnummern akzeptiert. SMS-Befehle von anderen Nummern werden dann ignoriert. Wenn Sie möchten, dass SMS Kommandos auch von anderen Absendern akzeptiert werden sollen, deaktivieren Sie diese Option.

Wenn man die Befehle korrekt verschickt, lösen sie am Zieltelefon keinen SMS Klingelton, kein Vibrieren oder sonst ein Zeichen für eingehende SMS aus. Darüber hinaus werden eingehende Befehls-SMS sowie Antwort-SMS von Anti-Theft nicht im SMS-Eingangs-/Ausgangsordner angezeigt.

Beachten Sie, dass bei falschem PIN die Befehls-SMS ignoriert wird und als herkömmliche SMS im Posteingang erscheint - samt üblicher SMS-Eingangsbenachrichtigung.

SMS-Befehlsübersicht

<i>VERLOREN</i>	Markiert das Gerät als VERLOREN. Dieser Befehl verursacht die gleichen Aktionen wie ein SIM Kartenwechsel, abhängig vom den Einstellungen zum Schutzverhalten.
Beispiel: 2222 VERLOREN	
<i>GEFUNDEN</i>	Markiert das Gerät als GEFUNDEN. Dieser Befehl deaktiviert die Telefonsperre und die Sirene.
Beispiel: 2222 GEFUNDEN	
<i>SPERREN</i>	Sperrt das Gerät.
Beispiel: 2222 SPERREN	
<i>ENTSPERREN</i>	Entsperrt das Gerät.
Beispiel: 2222 ENTSPERREN	
<i>NACHRICHT <Nachrichtentext></i>	Zeigt eine Nachricht am Gerät an. Eine derartige Nachricht kann aber einfach entfernt werden. Verwenden Sie SETZE SPERRTEXT um eine "permanente" Nachricht anzugeben, die angezeigt wird wenn das Gerät gesperrt ist. Dann benutzen Sie "SPERREN" um das Gerät zu sperren und die Nachricht anzuzeigen.
Beispiel: 2222 NACHRICHT Gib mir mein Telefon zurück!	
<i>SIRENE EIN</i>	Aktiviert die Sirene.
Beispiel: 2222 SIRENE EIN	
<i>SIRENE AUS</i>	Deaktiviert die Sirene.
Beispiel: 2222 SIRENE AUS	
<i>ORTEN</i>	Ortet das Gerät.
Beispiel: 2222 ORTEN	
<i>ORTEN <Intervall in Minuten></i>	Ortet das Gerät regelmäßig alle 5 Minuten.
Beispiel: 2222 ORTEN 5	
<i>ORTEN STOP</i>	Beendet eine regelmäßige Ortung.
Beispiel: 2222 ORTEN STOP	
<i>RUF AN [Telefonnummer]</i>	Wenn keine Telefonnummer angegeben wird, wird das Gerät Sie zurückrufen. Wird eine Telefonnummer angegeben, wählt das Gerät diese Nummer.
Beispiel: 2222 RUF AN	
Beispiel: 2222 RUF AN +43660333555	
<i>WEITERLEITUNG SMS [Telefonnummer]</i>	Wenn keine Telefonnummer angegeben wird, werden eingehende SMS unsichtbar an den Absender des Befehls weitergeleitet und beim eigentlichen Empfänger gelöscht (nicht zugestellt). Wenn eine Telefonnummer angegeben wird, werden eingehende SMS unsichtbar an die angegebene Telefonnummer weitergeleitet. Dieser Befehl überschreibt alle vorhergehenden SMS-Weiterleitungen. Die Weiterleitung kann durch den Befehl <i>WEITERLEITUNG SMS STOP</i> oder durch Öffnen von avast! Anti-Theft beendet werden.
Beispiel: 2222 WEITERLEITUNG SMS	
Beispiel: 2222 WEITERLEITUNG SMS +436603335551	
<i>CC SMS [Telefonnummer]</i>	Gleich wie WEITERLEITUNG SMS. Die eingehende SMS wird jedoch nicht gelöscht, sondern wird normal am Zielgerät empfangen (CC bedeutet Carbon Copy, Blaupause) Dieser Befehl überschreibt alle vorhergehenden SMS-Weiterleitungen.
Beispiel: 2222 CC SMS	
Beispiel: 2222 CC SMS +43660333555	

	Die Weiterleitung kann durch den Befehl <i>CC SMS STOP</i> oder durch Öffnen von avast! Anti-Theft beendet werden.
<i>CC ANRUF</i> [Telefonnummer]	Eingehende Anrufe an das Zielgerät werden über SMS-Benachrichtigung mitgeteilt. Die Benachrichtigungen werden an den Absender des Befehls geschickt, wenn keine Telefonnummer angegeben wurde, sonst an die angegebene Telefonnummer. Dieser Befehl überschreibt alle vorhergehenden SMS-Weiterleitungen. <i>Anrufe können nicht weitergeleitet werden, weil Anrufe vom Netzbetreiber weltweit unterschiedlich gehandhabt werden. Es ist auch nicht möglich, die Weiterleitung zuverlässig vor Dieben zu verstecken.</i> Die Benachrichtigungen können durch den Befehl <i>CC ANRUF STOP</i> oder durch Öffnen von avast! Anti-Theft beendet werden.
Beispiele: 2222 CC ANRUF	
Beispiele: 2222 CC ANRUF +43660222333	
<i>CC ALLE</i> [Telefonnummer]	Kombiniert die CC SMS und CC ANRUF Befehle. Dieser Befehl überschreibt alle vorhergehenden SMS- und Anruf-Weiterleitungen. Die Benachrichtigungen können durch den Befehl <i>CC ALLE STOP</i> oder durch Öffnen von avast! Anti-Theft beendet werden.
Beispiel: 2222 CC ALLE	
Beispiel: 2222 CC ALLE +43660222333	
<i>LÖSCHEN</i>	Löscht alle Daten vom Gerät
Beispiel: 2222 LÖSCHEN	
<i>ABFRAGE</i> <Abfragelimit> SMS	Abfrage der letzten 10 SMS Nachrichten
Beispiel: 2222 ABFRAGE 10 SMS	
<i>ABFRAGE</i> <Abfragelimit> EMPFANGENE SMS	Abfrage der letzten 10 empfangenen SMS Nachrichten
Beispiel: 2222 ABFRAGE 10 EMPFANGENE SMS	
<i>ABFRAGE</i> <Abfragelimit> 10 GESENDETE SMS	Abfrage der letzten 10 gesendeten SMS Nachrichten
Beispiel: 2222 ABFRAGE 10 GESENDETE SMS	
<i>ABFRAGE</i> <Abfragelimit> SMS FÜR <Telefonnummer>	Abfrage der letzten 10 SMS Nachrichten für die angegebene Telefonnummer
Beispiel: 2222 ABFRAGE 10 SMS FÜR +43660333555	
<i>ABFRAGE KONTAKTE</i>	Abfrage der Kontakte des Telefonbuchs
Beispiel: 2222 ABFRAGE KONTAKTE	
<i>ABFRAGE PROTOKOLL</i> <Abfragelimit>	Abfrage des Anrufs- und SMS-Protokolls.
Beispiel: 2222 ABFRAGE PROTOKOLL 10	

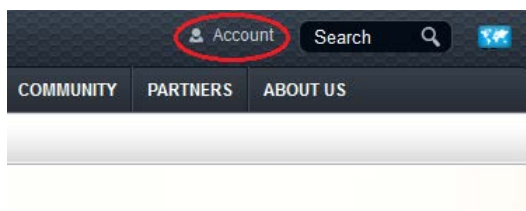
STARTEN	Startet die avast! Anti-Theft Benutzeroberfläche
Beispiel: 2222 STARTEN	
BEENDEN	Beendet die avast! Anti-Theft Benutzeroberfläche
Beispiel: 2222 BEENDEN	
NEUSTART (nur für gerootete Installationen)	Startet das Gerät neu
Beispiel: 2222 NEUSTART	
SETZE BESITZER <Name des Besitzers>	Ändert den Namen des Geräte-Besitzers
Beispiel: 2222 SETZE BESITZER Charles Chaplin	
SETZE PIN <PIN>	Ändert den avast! PIN. Der PIN muss aus 4-6 Ziffern bestehen.
Beispiel: 2222 SETZE PIN 3333	
SETZE FREUND 1 <Telefonnummer>	Ändert die Telefonnummer des ersten Freunds. Geben Sie eine gültige Telefonnummer an
Beispiel: 2222 Setze FREUND 1 +436601222092	
SETZE FREUND 2 <Telefonnummer>	Ändert die Telefonnummer des zweiten Freunds. Geben Sie eine gültige Telefonnummer an
Beispiel: 2222 Setze FREUND 2 +436601222092	
SETZE NURFREUNDE 1	Ändert den SMS-Autorisierungsmodus (0 = alle Nummern erlauben, 1 = nur Freund-Befehle erlauben)
Beispiel: 2222 SETZE NURFREUNDE 1	
SETZE SPERRMODUS <Sperrmodus>	Ändert das Sperr-Schutzverhalten des Telefons (0 = nicht sperren, 1 = automatisch sperren)
Beispiel: 2222 SETZE SPERRMODUS 1	
SETZE SIRENENMODUS <Sirenenmodus>	Ändert das Sirenen-Schutzverhalten (0 = keine Sirene bei Sperrung, 1 = Sirene bei Sperrung)
Beispiel: 2222 SETZE SIRENENMODUS 1	
SETZE ANWENDUNGSSPERRMODUS <Anwendungssperr-Modus>	Ändert das Anwendungsmanager und Einstellungs-Schutzverhalten (0 = kein Schutz, 1 = Programm-Manager verhindern, 2 = Alle Einstellungen verhindern)
Beispiel: 2222 SETZE ANWENDUNGSSPERRMODUS 1	
SETZE USBSPERRMODUS <USB-Sperr-Modus> (nur für gerootete Installationen)	Ändert das USB-Debugging-Schutzverhalten (0= USB Debugging erlauben, 1 = USB Debugging sperren)
Beispiel: 2222 SETZE USBSPERRMODUS 1	
SETZE DATENVERBINDUNGSMODUS <Daten-Modus> (nur für gerootete Installationen)	Ändert das Datenverbindungs-Schutzverhalten (0 = keine Datenverbindung erzwingen, 1 = Datenverbindung erzwingen)
Beispiel: 2222 SETZE DATENVERBINDUNGSMODUS 1	

SETZE AKKUSMSMODUS <Akku-Modus>	Ändert das Akku-Schutzverhalten (AUS =niemals benachrichtigen, EIN = bei niedrigem Akku-Stand benachrichtigen, wenn das Gerät als verloren markiert ist oder eine nicht vertrauenswürdige SIM Karte eingelegt ist, IMMER = bei niedrigem Akku-Stand benachrichtigen, auch wenn das Gerät nicht als verloren markiert ist)
Beispiel: 2222 SETZE AKKUSMSMODUS EIN	
SETZE SPERRTEXT <Sperrtext>	Ändert den eigenen Sperrtext
Beispiel: SETZE SPERRTEXT Bitte um Rückruf unter +4313283483	
SETZE AUTOGPS <GPS-Modus>	Ändert die Einstellung zur automatischen Aktivierung von GPS (0 = aus, 1 = ein)
Beispiel: 2222 SETZE AUTOGPS 1	
SETZE LÖSCHMODUS <Lösch-Modus>	Gründliches Löschen ein- oder ausschalten (0 = aus, 1 = ein)
Beispiel: 2222 SETZE LÖSCHMODUS 1	
SETZE SCHUTZ <Schutz-Modus>	Schaltet den Anti-Theft Schutz ein oder aus (0 = aus, 1 = ein) Warnung: Wenn Sie den Befehl ausführen können Sie avast! Anti-Theft komplett ausschalten und der Anti-Theft Schutz wird funktionsunfähig.
Beispiel: 2222 SETZE SCHUTZ 1	

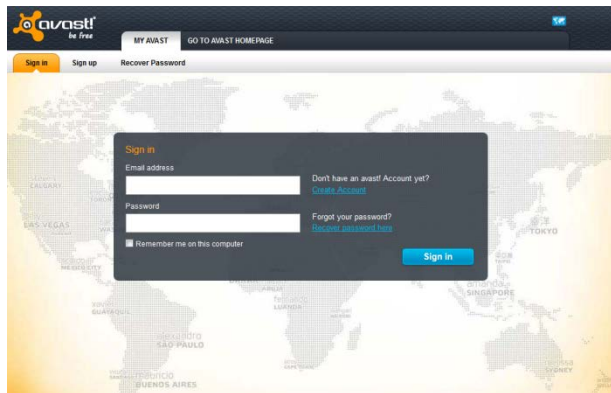
avast! Account Internetportal

Wenn Sie einen avast! Account registriert haben, können Sie im my.avast.com Internetportal Ihre Einstellungen ändern. Wenn Sie auch avast! Anti-Theft installiert haben, können Sie auch bei Verlust oder Diebstahl vom Portal aus Kommandos an das Gerät schicken. Das funktioniert nicht nur auf Handys, sondern auch auf Tablet und Geräten ohne SIM-Karte, sofern sie eine Internetverbindung haben.

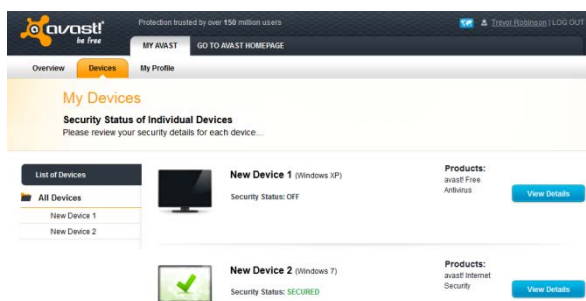
Sie können Ihren persönlichen avast! Account im Verlauf der Installation erstellen oder später in den Einstellungen von avast! Mobile Security bzw. Anti-Theft. Wenn Sie noch keinen avast! Account haben, ist die Erstellung eines neuen sehr einfach. Öffnen Sie einfach die avast! Webseite und klicken Sie auf "Account" bzw. "Konto" rechts oben.



Am nächsten Bildschirm geben Sie bitte Ihre eMail-Adresse und ein Passwort an um den Account zu erstellen. Sie erhalten eine eMail und bestätigen darin Ihre eMail-Adresse durch einen Klick auf den Aktivierungslink.



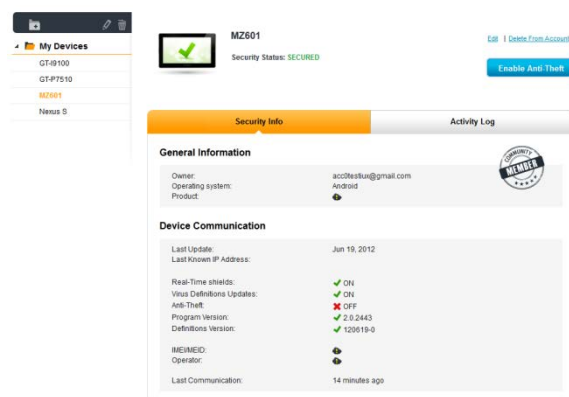
Wenn Sie sich nun einloggen, sehen Sie den Status all Ihrer Geräte, die von avast! geschützt werden.



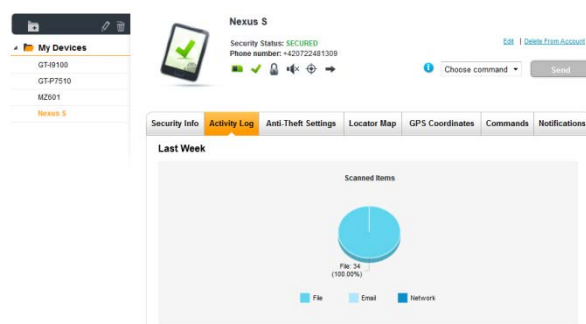
Um sicher zu stellen, dass der Status Ihrer Geräte online immer korrekt ist, muss "Status melden" in den avast! Accounteinstellungen am Gerät aktiviert sein.

Um Zugriff auf die Einstellungen und Fernsteuerungsfunktionen zu erhalten, wählen Sie bitte ein Gerät aus der Liste "Alle Geräte".

Im Tab "Sicherheit" sehen Sie Informationen zu Ihrem Gerät und dem Status verschiedener Sicherheitsfunktionen.

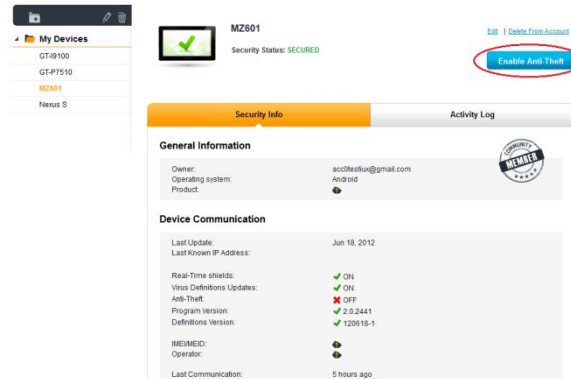


Das Aktivitätslog zeigt eine Übersicht über die vergangenen Scans in der vergangenen Woche, Monat bzw. Jahr.

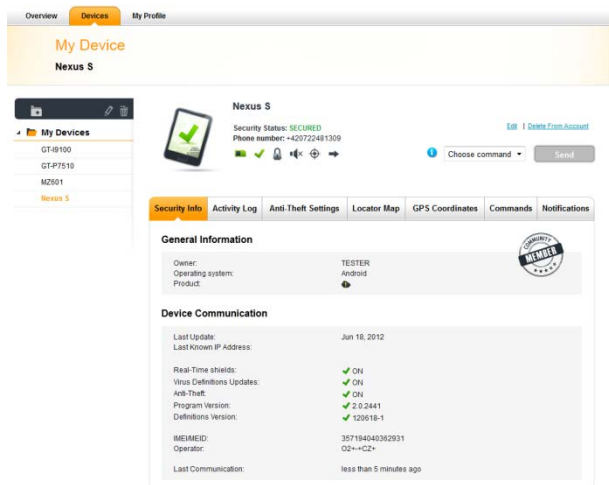


Um die Anti-Theft Fernsteuerungsoptionen nutzen zu können, muss Anti-Theft am Gerät aktiviert sein. Wenn es das nicht ist, wählen Sie "Anti-Theft Einschalten". Beachten Sie, dass Anti-Theft nur aktiviert werden kann, wenn es auch am Gerät installiert ist. Ferninstallation ist nicht möglich.

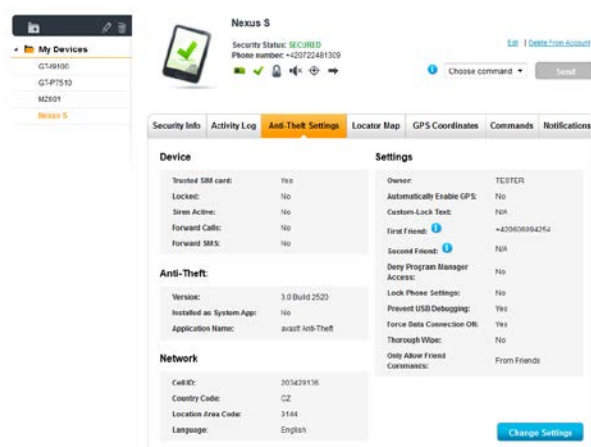
Um Anti-Theft zu aktivieren, drücken Sie bitte den blauen Knopf:



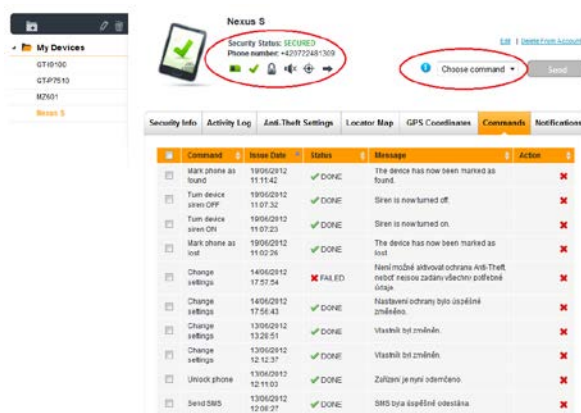
Ist Anti-Theft aktiviert, sehen Sie einige zusätzliche Tabs in denen Sie Ihr Gerät konfigurieren können, Kommandos senden sowie vom Gerät empfangene Informationen angezeigt bekommen wie Ortungsdaten und andere Benachrichtigungen.



Im Anti-Theft Tab können Sie mit dem Button "Einstellungen" die Einstellungen Ihrer Anti-Theft Installation ändern.

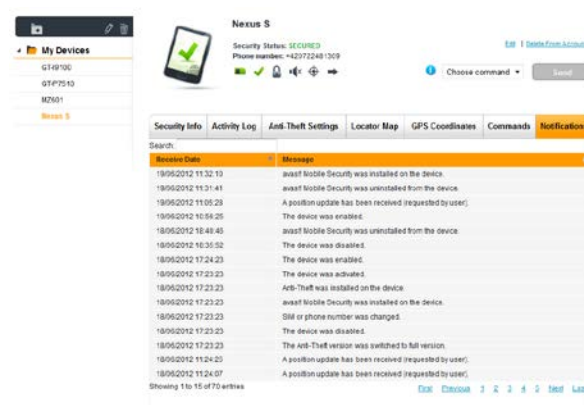


Im Tab "Befehle" sehen Sie eine Übersicht der Kommandos die an Ihr Gerät geschickt wurden. Von Ihrem avast! Account aus können Sie Befehle an Ihr Gerät schicken, wie es sonst auch von anderen Mobilgeräten aus möglich wäre. Wählen Sie einen Befehl aus der Drop-Down-Auswahlliste, wählen Sie "Senden" und ein Fenster geht auf, in dem Sie weitere Parameter spezifizieren können, bevor das Kommando gesendet wird.

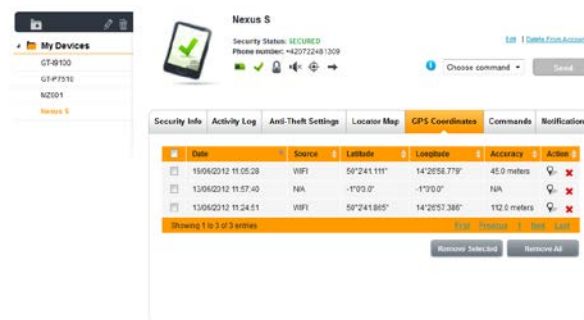


Sie können auch die Shortcut-Icons im oberen Fensterbereich verwenden um das Gerät als "Verloren" zu markieren, es zu sperren, die Sirene zu aktivieren, zu Orten und um die Weiterleitung von Anrufen/SMS zu aktivieren.

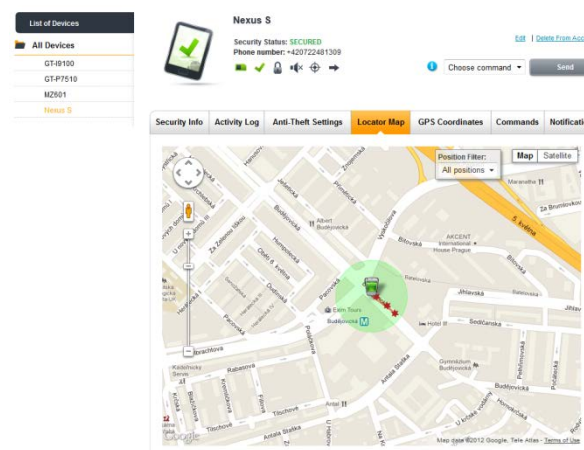
Im Tab "Benachrichtigungen" sehen Sie Informationen die von Ihrem Gerät empfangen wurden. Zum Beispiel Informationen über SIM-Kartenwechsel und Ortungsdaten.



Wurde eine Ortung vom Gerät empfangen, finden Sie detaillierte Informationen im Tab "GPS Koordinaten".



In der "Ortungsübersicht" sehen Sie alle empfangenen Ortungen auf einer Karte dargestellt. Jede Position wird als roter Stern mit einem grünen Kreis dargestellt. Klicken Sie auf einen roten Stern um Details wie Datum, Zeit und Genauigkeit der Ortung in Metern zu erfahren. Die Genauigkeit wird durch die Größe des grünen Kreises repräsentiert.



**Vielen Dank, dass Sie sich für
avast! entschieden haben.**

